



Privacy & Security—Are They Irreconcilable Interests?

**Privacy and Security: Seeking a Middle Path
5th Annual CACR/Ontario IPC
Privacy & Security Workshop
October 28-29, 2004
University of Toronto**

**David Loukidelis
Information and Privacy Commissioner for British Columbia**

October 27, 2004

I'm very grateful to be here today to speak to such a distinguished group and thank my good friend and colleague, Ann Cavoukian, for being kind enough to invite me here to speak to you.

I'm afraid, however, that I'm going to let you down, at the very least because I cannot in any meaningful way, for reasons I'll explain in a moment, substantively address the topic the program says I'll deal with. You'll see in the program for today that my remarks are billed as being about the USA Patriot Act and the outsourcing—the program may refer to it as offshoring—of personal information.

This is topical, of course, in light of the USA Patriot Act, whether we're talking about outsourcing of data as part of the outsourcing of government services or data outsourcing in the ordinary course of business. The USA Patriot Act is, of course, a significant US law signed into law by President Bush on October 26, 2001, three years ago on Tuesday, after rapid and almost unanimous passage in both Houses of Congress. Here in Canada, we passed similar and far-reaching legislation less than two months later, in the form of the ATA. Since then, we've passed several new laws that are of a piece with the USA Patriot Act in many ways—I'm thinking here of the Customs Act amendments of a few years ago that allow Canadian authorities to share personal information of travellers for a wide range of purposes (we were told these span law enforcement through to public health uses), the Public Safety Act passed in May of this year that allow information sharing for national security and law enforcement purposes, and amendments to our federal private sector privacy law, the Personal Information Protection and Electronic Documents Act, passed earlier

this year, that allow private sector organizations to disclose personal information to authorities for national security purposes without notice to or the consent of customers. We've also heard about the federal government's plans for a no fly list.

These laws have been passed with the aim of investigating and deterring terrorist acts in Canada. I don't think anyone here today would deny that, whatever you think of the USA Patriot Act—and I express no views on the merits of that law as a US law applying in the US, since it's none of my business—that law has been controversial in the US, just as the Canadian post-9/11 laws I've just mentioned have been controversial here.

The province of British Columbia's government has, since late 2001, been pursuing a policy of outsourcing public services to private sector contractors. And it was alleged earlier this year that, if a US linked service provider had custody of personal information of BC citizens, even in Canada, a secret order might be made under the FISA as amended by the USA Patriot Act and could reach across our friendly border and seize that information.

A great deal of public debate followed this allegation, which was actually part of a lawsuit against our government that is ongoing, and ultimately in the face of great interest and concern, in May of this year, I initiated as public and transparent a process as possible in order to get the widest possible input on two questions.

First, does the USA Patriot Act permit US authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of US-linked private sector service providers? If it does, under what conditions can this occur?

Second, if it does, what are the implications for public body compliance with the personal privacy protections in FOIPPA? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with FOIPPA?

We received over 500 submissions in response to these questions. This was, to me, an overwhelming response. These submissions went far beyond the two technical questions I'd asked. They raised fundamental questions around national sovereignty for Canadians national security and privacy—to give only a few.

We were driven to consider much more than the USA Patriot Act and its effect here in Canada. We had to, truly had to, confront a number of vexing issues to do with the nature of privacy and its importance in our democracy. We confronted the fact that, as national security continues to dominate the public policy agenda here, in the US and elsewhere, the lines between national security and ordinary law enforcement activities seem to be blurring in Canada and elsewhere. We came to understand that many citizens live in a state of fear day by day, in a state of apprehension that has us primed for the next attack from Outside, from the Other, and that this climate of fear means there is continued risk for our democracy.

This process of analysing foreign law and its implications in Canada has been both vexing and fascinating. My report on the privacy implications of the USA Patriot Act in British Columbia will be released tomorrow, along with my comments on the BC government's recently passed legislative fix regarding the USA Patriot Act. The delayed release of my report means I can't talk to you today in any meaningful way about our analysis of the USA Patriot Act and its impact in Canada—though I will say there is clearly an impact—and I hope you and Ann will forgive me for not directly addressing the USA Patriot Act as suggested in the program.

However, I can say that our work on the USA Patriot Act—this is really stating the obvious—has affirmed very clearly how much, since 9/11, public policy debate and discourse have shifted worldwide. We are in a war on terror, widely spoken of as such—and as an aside, I'll leave it to international lawyers, military experts and historians to decide whether the characterization of what's going on as a war by any description, old or new, is accurate.

Whatever the label we give to the new policy imperative, however, it's clear that the arena of debate, the thrust of public discourse and policy action, has shifted dramatically in just three years. Although it may have diminished somewhat since 9/11, people seem to continue to support significant changes in policy, law and action, all in the name of national security and the war on terror. This state of affairs is born of fear—we are afraid, we feel insecure, fear that we are not safe.

In this context, I'd like to spend a few minutes today to address, in a necessarily superficial way, what we mean by security and why we have to think about it more rationally than we might be tempted.

Let me shift gears for a second and conduct a straw poll of sorts about security.

First, let me see your hands up—way up high—if you *feel* secure sitting here today? OK, that's about 80% of you.

Let me see your hands—high up—if you think that you *know* beyond a doubt that you are completely secure sitting here today. That's about 10% of you.

Next, how many of you either feel or know, for sure, that you're *less*—not more—secure today than you were before 9/11? For the roughly 25% of you who believe you're more vulnerable now than you were before 9/11, your belief raises some questions.

Does your perception of increased vulnerability stem from *certain* knowledge that you are, *factually*, less safe? Or does your perception of vulnerability refer to a state of mind in which you *feel* less protected for reasons you find it difficult to identify or quantify?

Now, can someone tell me how many people of all nationalities have been killed worldwide by terrorism of all kinds in the 8 years between 1996 and 2003? According to the US State Department, some 6,800 people of all nations have been killed and some 17,000 have been wounded. Just about 45% of those killed died in the 9/11 attacks. I don't need to compare these numbers of deaths to, say, the numbers of people killed each year in Canada—let alone over 8 years—in car accidents or by cancer. Each death due to terrorism is both tragic and unacceptable, but the relatively small number of deaths due to terrorism—just over 800 a year worldwide—illustrates the power of fear. These figures reinforce how seismic a shift there has been in the policy debate since 9/11.

I've asked you about your perceptions or beliefs about security and safety because I'm concerned that in recent years—especially since September 11—our public discourse has tended to assign great, and sometimes almost super-ordinate, value to 'security' and 'safety', but without necessarily approaching those questions rationally. Our political leaders and pundits commonly speak of the need to maximize security—to protect us from harm—and in doing so they usually explicitly characterize the security imperative as being driven by risks of harm from terrorist acts.

Now, I'm not for one second suggesting that law enforcement and security agencies shouldn't be trying to protect us from terrorism—that's their job and I'm grateful to them for doing it. Each death due to terrorism is lamentable, is unacceptable.

Nor am I implying that everything is the way it was before 9/11. That would be a silly thing to suggest, as there is clearly a desire to attack again and to inflict even greater harm. What I am suggesting, however, is that the current focus on security generally must account for actual risk, and failure to do so in turn has significant implications for how we assess security risks and for the actions we take to enhance security.

Our failure to define what we mean by security, and what it means for our lives individually and as a society, means that our assessments of security threats are prone to both unintentional and, dare I say it, intentional distortion. And distorted analysis can—however it may be motivated—have potentially serious implications for our safety, on the one hand, and for our privacy and other rights and freedoms. My point is we must be as dispassionate, as politically disinterested, and as rational as possible in assessing security risks, in considering measures to enhance security, and in analyzing their inter-play with our rights and freedoms.

Let me first re-state the question I asked each of you to answer a minute ago—does 'security' for you mean a state of being in which an individual is protected against physical harm? Is it a state of being where she's at ease, where she's free from worry? More likely, without thinking about it, we perceive 'security' as blending each of these concepts—we see 'security' as a state in which our bodies *and* our minds are safe and at ease. This is to state the obvious, since how we feel is to greater or lesser degrees connected with our knowledge of the risk of physical peril, our awareness that we or are not physically safe.

Many, perhaps most, of us would agree that we should, as a society, try to optimize both the feeling and the actuality of security. The rub, of course, is that it's possible to *feel* less secure even though we're not, and the converse is also true. We can only make individual judgements about our level of our security—or that of our loved ones—based on the information we have about our world and the risks it presents.

Obviously, to learn about the world around us, we depend on information that we glean from sources ranging to casual conversation to academic works. And, depending on the quality of that information, it's entirely possible for us to feel or believe that we are more vulnerable, believe we are less secure and are subjected to risk, even when we're not.

Let me give you one example from my work as a privacy commissioner. I've on many, many occasions had to respond to those who support increased police surveillance of our streets because crime rates in Canada are, they know or think they know, climbing ever higher, with our communities descending further and further into lawlessness.

Perhaps this is due, in part, to the fact that we are, if we want to be, constantly bathed in violence on TV, often in the form of true-life crime shows that depict, in graphic detail, the most gruesome imaginable murders. Even if these crimes happened years ago in a remote part of the US, as is often the case, the horror is projected right into our homes, our most private places, here and now. And when we turn on the news, surf the Internet or read the newspaper, we have instant—often literally graphic—access to information about murders and atrocities around the world. Could it be that this diet of crime and violence is part of what makes us feel less safe? I think it is, though I should be clear that I'm *not* blaming the media for our problems—after all, we get what we ask for.

But are we allowing this information and entertainment to distort our perceptions of risk? As for Canadian crime and the perception that violence is epidemic, the actual statistics tell a different tale. Year after year since 1991, violent crime has gone down in Canada. There was a noticeable spike upward in the 1970s, as we Baby Boomers grew into our violent years, but violent crime has generally been trending down for over a decade. The last time I checked the statistics, violent crime was more than 20% lower than it was in 1991 and was still heading down.

So, in Canada, at least, many of us fear that we're less secure, and that a tide of violence is about to engulf us, but the numbers generally mean that our perception squares with reality TV but not reality. Yet many of us support more scrutiny, more surveillance of the population, greater law enforcement powers, because we *feel* less safe against all evidence.

The UK offers a good example of how feelings about safety can override the evidence. Polls there have pretty consistently shown that a clear majority of the

British public accept the pervasive video surveillance that exists there. Violent crime in the UK is not decreasing as it is here—it has actually increased in recent years in many areas, leaving one to wonder, as an aside, how well video surveillance is working, if it's working at all (something even Home Office studies have questioned). Yet the efficacy of all this routine surveillance doesn't seem to matter, since a majority of Britons have also told pollsters they like video surveillance simply because it makes them *feel* safer. Small wonder, you might think, that the British government has in this light spent hundreds of millions of dollars on politically-popular surveillance. The same risk of, quite frankly, garbage-in garbage-out public opinion exists post-9/11 in Canada and elsewhere if we don't make sure that we each have relevant and reliable information on which to base our assessments of risk and thus new laws and policies.

Returning to my theme, it is crucial after 9/11 that decision-makers not abdicate their responsibility to, as disinterestedly as possible, do three things. First, our elected representatives—they work for us, after all—must focus on real threats and assess real risk. Second, they must at all times act on the knowledge that risk can never be eliminated. Third, they must act on the principle that pandering to fear, much less creating the conditions for it to flourish, are not acceptable in a free and democratic society.

More specifically, national security measures—ranging from terrorist threat level warnings to routine surveillance of the general population—must never be implemented only to make people *feel* more secure. The public's *comfort* would not by any stretch be sufficient reason, for example, for Parliament to enact the Draconian national security laws that were hastily passed immediately after 9/11. The *appearance* of quick action that such laws communicated to Canadians—making us *feel* like something was being done to protect us—would not be an acceptable motive for these laws.

Jeffrey Rosen argues in his latest book, *The Naked Crowd*, that democracies have become or are becoming risk averse. As he points out, much of this has to do with human psychology—with our tendency to let fear of the unknown over-ride rational assessments of risk. When our conclusions as to risk are increasingly based on bad information—such as mistaken perceptions of crime—or on information that we are told exists but which must remain secret and unquestioned—human nature will tend towards fear and towards feelings of insecurity.

And why wouldn't a politician be tempted, quite rationally, to pander to that? Power would, in such an environment, increasingly depend on their instituting measures popularly felt to make us more secure from what we think may be growing crime rates or imminent threats of terrorism.

Maybe it's an impossible thing to expect—I hope and truly believe not—but our leaders must have the courage to resist, at all times, any instinct for their own short-

term political advantage when they assess the need for, and fashion, security laws and measures.

My purpose here is not to be cynical or jaded—far from it. Rather, I'm concerned that we've created, or are at risk of creating, a false dichotomy—between insecurity and fear, on the one hand, and security and comfort, on the other. Give us comfort and peace at all costs, many of us ask—watch over me, keep me safe. But has anything ever been certain in life? We don't need to fall into an abyss of despair to recognize that nothing is for sure, that there's always risk in life, that we can't take anything in life for granted. Are we somehow forgetting these basic facts of life when it comes to fear, and perceptions of risk, around terrorism and crime?

We mustn't move too far down the road of increased surveillance and security—it's always tough to strike the balance, I know—because of inordinate fears and distorted understandings of actual risk. To protect our rights and freedoms in Canada, we have to keep it clearly in view that our steps toward greater security can have a long-term impact on our freedom, without there necessarily being any benefit in terms of better or more security. If we yearn to find 'security', therefore, we've got to constantly question what it means and we must always remember that, whatever we are seeking, we risk a great deal for ourselves and the kind of society in which our children will live. Freedom is about risks, and the more freedom you give to people, the greater the risks. The more we try to maximize security, the more we're likely to curtail freedom.

We also have to remember the temptations of power and the utility of fear, something to which I've already alluded. To reinforce this point, I'd like, with your indulgence, to quote at some length from Reg Whitaker, a Canadian privacy and security academic, on this issue:

National security, or national *insecurity* to be more precise, is an anxiety that afflicts states across the ideological spectrum. Intelligence in the service of domestic political policing has been used by governments of all persuasions, and every type of state has relied at least from time to time on secret or political police against the perceived threat of subversion, if not revolution ... [H]owever different the texture of domestic intelligence in different regimes, it is the universality of the phenomenon in the twentieth century that is most arresting. The tools for internal surveillance and control being available, no state has resisted the temptation to use them, and few have not attempted to refine the tools yet further. States with many external and internal enemies, real and potential, have often used these tools recklessly and brutally; states with higher degrees of domestic consensus have most often used the tools with greater restraint, discretion, and skill, usually during periodic bouts of national or state insecurity. Such relative restraint, however, has served to mask the negative effects of secret political policing on the practice of liberal democracy.

Fears for internal security and of enemies within tend to be sparked in the first instance by international insecurity. The pathologies of counterintelligence, described above, are intimately linked to the perception of the enemy within as

an insidious extension of the enemy without. The "fifth columnist." The spy, the saboteur, the foreign-directed terrorist or subversive: these are images that draw their menace, and fascination, from the blurring of Inside and Outside, of Us and Them. The Cold War image of "reds under the bed" captures this anxiety indelibly. Xenophobia, ideology, and sexual/cultural panic all reinforced one another.¹

Now more than ever, it's critical that governments not enact any rights-curtailling laws or adopt freedom-limiting security measures simply because they make people feel more secure without actually making them more secure. And even if there's a security enhancement, it's incumbent on governments—applying the usual constitutional tests—to demonstrate that the measure is clearly justified and that its security benefits outweigh the harm to our rights and freedoms.

Let me give you an example of a security measure that will, if implemented, jeopardize privacy and other rights but without any clear benefit in terms of increased security. My example is the recently announced Canadian no fly list. In making this announcement, the federal government did not say how the list would be created, on what information it would be based or how underlying assessments of the risk presented by individuals would be carried out. Nor was there any indication that someone on the no fly list would have any right to complain, to find out how she or he got onto the list, how an individual could ask to have errors corrected. In short, there was no indication that the federal government had any intention of following the fair information practices that have been internationally recognized for over 30 years. Both Ann Cavoukian and I wrote to our federal colleague, Jennifer Stoddart, the Privacy Commissioner of Canada, expressing concern about this, and I know Jennifer has taken this up with the federal government.

Another area of risk to privacy and other rights can be seen in the trends toward the merging of public and private sector data—including credit-rating information and government watch lists—for analysis for national security reasons. The suggestion in such cases tends to be, it seems, that the data mining software will predict that you may be a terrorist or, to use, the generous language of Canada's Canadian Security Intelligence Service Act, a threat to the security of Canada (including due to your actions that are considered "detrimental to the interests of Canada").

Now, data mining can be beneficial, but I'm concerned about its use in ways that generate new information about individuals where the new information is used to make decisions that affect those individuals directly. Others here today can argue much more knowledgeably about the dangers of using data mining to identify much less capture real or would-be terrorists—the inaccuracies in so much of the data that are likely to be used and the false positives or negatives such systems generate are all up for debate. Also up for debate is the fact that if we come to rely too much on

¹ Reg Whitaker, *The End of Privacy: How Total Surveillance Is Becoming A Reality* (New York: New Press, 1999) at 19-20.

this kind of technology, we may pay a high price if we come to trust the products of data mining too much.

If they're adopted, systems like this, it seems to me, promise only one thing for certain—we'll all be under surveillance and many of us will be wrongly presumed to be guilty or at least suspected of something. These systems offer the prospect of one thing for certain, everyone's privacy will be invaded and in potentially open-ended ways. And large collections of primary data—and the secondary information derived using data mining techniques—will be too rich a resource for either criminals or governments to long resist exploiting somehow, sometime. As my predecessor David Flaherty has demonstrated in his comparative work on surveillance societies, the phenomenon of function creep—whether official or illicit—is a law of data protection as absolute as any law of nature. Data collected for one purpose will always find another purpose and that as yet unascertained other purpose could well have profound effects on our privacy and other rights.

In closing, I readily agree that technology can be designed to work for security and privacy. Take the example of biometrics, which, when properly deployed, can improve identification, as I suggested to the Parliamentary Standing Committee on Citizenship and Immigration last year in urging it not to recommend a new national ID card. Technology can, of course, help reconcile security and privacy if we approach the issues rationally and clearly.

But we have to *require* decision-makers to clearly define what they mean when they cite the security imperative as prevailing over all else. We have to require them to assess risk realistically and meaningfully, unswayed by either our own fears or their own political or career interests—and I say this recognizing it's a very tall order.

We have to require decision-makers to be clear-eyed about technology, to adopt only those technologies that actually address real security risks and to do so in ways that, as far as possible, build in privacy protections.

Technology is a tool, though we are often too ready to ascribe magical healing powers to it. It's not up to technology to reconcile privacy, security and identity—it's up to us, using good old-fashioned policy-making methods.

Thank you so much for your time.

* * *

